

# DIREITO DIGITAL: UMA ANÁLISE PREPoderante SOBRE O MAIS NOVO RAMO DO DIREITO E SUAS TRANSFORMAÇÕES SÓCIO-JURÍDICAS

Elisa Mariano da Silva<sup>1</sup>

Nathália Guariento<sup>2</sup>

Rafaele Oliveira Queiroz<sup>3</sup>

Thamires Resende<sup>4</sup>

Cristian Kiefer da Silva<sup>5</sup>

**RESUMO:** O presente artigo apresenta um estudo sobre o novíssimo ramo do Direito, surgido a partir da necessidade de se regular e disciplinar as relações jurídicas ocorridas no ambiente virtual, relações estas cada vez mais presentes na vida de todos; o Direito de Informática. No que diz respeito às infrações ocorridas por meio da internet, a legislação brasileira jurídico-penal ainda é incipiente, não tutelando todos os bens jurídicos ameaçados com a utilização da TI, (Tecnologia da Informação). Contudo, esse fato não impede o desenvolvimento do trabalho dos órgãos competentes em articular ações no enfrentamento dessa nova modalidade delitiva. Nesse sentido, o presente estudo aborda como deve ser a procedência das vítimas frente aos cibercrimes e apresenta propostas de uma utilização adequada da rede. Outrossim, é elencada a questão midiática que envolve o acesso a internet e sua conseqüente repercussão social. Lado outro, preocupa-se em abordar as consequências da participação de um número cada vez maior de pessoas sem a devida informação nas conhecidas redes sociais, meio atualmente utilizado na coleta de dados para fazer vítimas, devido ao fácil acesso às informações publicadas.

**PALAVRAS-CHAVE:** DIREITO DE INFORMÁTICA. REDES SOCIAIS. CIBERCRIMES.

**ÁREA DE INTERESSE:** Direito Penal

---

## 1 INTRODUÇÃO

A internet, desde a sua existência, tem contribuído para o desenvolvimento da sociedade através, sobretudo, do rompimento de barreiras - da informação, da distância, do conhecimento, de pré-conceitos, das relações afetivas, inclusive - a passos largos. Concomitantemente a essa mudança, a internet é utilizada para a prática de atos ilícitos. É nesse contexto que o presente trabalho procura abordar alguns pontos do novíssimo ramo do Direito - o Direito de Informática - surgido a partir da necessidade de regulamentar as relações virtuais.

Sob o foco do Direito Penal Informático, será abordado logo mais as características dos chamados *cibercrimes* ou crimes de informática: as condutas classificadas como crimes próprios e impróprios de informática, o criminoso digital como o sujeito ativo, a atuação dos órgãos competentes na resolução desses casos.

Ademais, é abordado um tema que está em voga, qual seja, o cometimento de crimes por meio das redes sociais. As espécies de redes sociais, suas peculiaridades, as conseqüências do mau uso na transmissão de informações por meio dessa rede de pessoas e o uso adequado dessa nova forma de comunicação.

Sob a perspectiva da Constituição Federal Brasileira, são elencados direitos inerentes e invioláveis ao indivíduo, quais sejam o direito à intimidade e o direito à privacidade, garantias

estas que estão sendo limitadas com a utilização exacerbada da liberdade de expressão *online*.

## 2 A INTERNET

### 2.1 Conceito

A Internet, segundo lição de Fabrizio Rosa, “consiste num conjunto de tecnologias para acesso, distribuição e disseminação de informação em redes de computadores” (ROSA, 2002). Acrescenta-se que não só a informação é disseminada por esta rede, mas também entretenimento, comunicação, relações jurídicas, comerciais, afetivas e tantas outras que o ser humano é capaz de desenvolver.

Segundo Patrícia Peck Pinheiro, “a Internet é mais um meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de Indivíduos” (PINHEIRO, 2008).

A internet representa, sem dúvida, um incrível avanço tecnológico. Mas muito mais que isso, ela representa também um rompimento de fronteiras, um encurtamento de distâncias, uma democratização de conhecimento, tudo isso sem que se perca a autonomia das identidades. Com efeito, se de um lado a globalização se manifesta tão favoravelmente através da internet, lado outro a rede se torna um moderno e eficaz meio de se cometer atos ilegais.

## 2.2 Breve histórico

A Internet, conforme elenca o mencionado autor, é comumente designada World Wide Web - www e está completando cerca de duas décadas de existência (ROSA, 2002). “Ela foi criada nos Estados Unidos da América, no final dos anos 60, como um projeto militar que buscava estabelecer um sistema de informações descentralizado e independente de Washington, para que a comunicação entre os cientistas e engenheiros militares resistisse a um eventual ataque à capital americana durante a Guerra Fria” (ALMEIDA, 1988).

Conforme mencionado, a internet foi concebida no contexto da Guerra Fria, época em que a criação de inovadoras estratégias de combate se faziam extremamente necessárias. Conforme leciona Fabrizio Rosa, em 1957, quatro meses após a União Soviética por em órbita o primeiro satélite espacial, (o Sputnik), os Estados Unidos da América anunciavam a criação de uma agência federal norte-americana cujo objetivo era pesquisar e desenvolver alta tecnologia para as forças armadas (ROSA, 2002).

“Essa agência era conhecida como ARPA - *Advance Research Projects Agency*, que durante os anos 60, foi aperfeiçoada no intuito de sobreviver a um possível bombardeio, de modo a permanecer ativa e a possibilitar o tráfego de informações aos seus destinatários. Era a ARPANET, (rede de agência de projetos avançados de pesquisa)” (ROSA, 2002).

Nos anos 70, “a internet passou a ser utilizada para fins acadêmicos e científicos. O correio eletrônico, até hoje a aplicação mais utilizada da rede, foi criada em 1972 por Ray Tomlinson. Em 1973, Inglaterra e Noruega são ligadas à rede, tornando-se, com isso, um fenômeno mundial. Em meados da década de 80, o governo estadunidense abriu a rede às empresas e continuou financiando a ARPANET até o ano de 1989, quando também foi lançado o primeiro browser (*Windows*); tendo sido apresentado em Genebra a *World Wide Web* (ROSA, 2002).

Com efeito, “foi a www ou W3 (malha mundial ou teia de alcance mundial) a responsável pela popularização da internet, o que permitiu à rede crescer em taxas vertiginosas. Outrossim, em 1990, entra no ar o primeiro provedor de acesso comercial do mundo, o *World*, permitindo que usuários comuns acessassem a grande rede a partir de um micro e de um *modem*” (ROSA, 2002).

## 2.3 Regulamentação da Internet no Brasil e no mundo

As primeiras normas que visavam regular o serviço de internet foram traçadas em 1995, em nota conjunta do Ministério das Comunicações e do Ministério da Ciência e Tecnologia. Estabeleceu-se, por exemplo, que os serviços comerciais da rede seriam fornecidos por empresas privadas.

Sabe-se que não há uma legislação penal especial e autônoma para regulamentar os crimes cometidos na rede. O que ocorre, então, é uma adaptação da atual parte especial do Código Penal. Mas é importante salientar, conforme lembra Fabrizio Rosa, que “não se deve confundir um crime comum praticado pelo uso ou contra o computador de um “crime de informática” propriamente dito”. Daí a necessidade de uma legislação específica para esses delitos: “ao formular uma nova categorização, o legislador atrai a atenção da indústria, do mundo acadêmico e do governo para o fato em si que, então, se torna objeto de aprofundada reflexão jurídica e técnica” (ROSA, 2002).

Nesse sentido é que defende-se uma legislação específica para estes novos comportamentos não previstos pelo legislador de 1940, haja visto terem surgido com o advento da internet.

Com efeito, há algumas leis no ordenamento jurídico brasileiro que disciplinam o uso da internet. À exemplo, a Lei 7.232, de 29 de outubro de 1984, que “estabelece princípios, objetivos e diretrizes da Política Nacional de Informática, seus fins e mecanismos de formulação, cria o Conselho Nacional de Informática e Automação - CONIN, dispõe sobre a Secretaria Especial de Informática - SEI, cria os Distritos de Exportação de Informática, autoriza a criação da Fundação Centro Tecnológico para Informática - CTI, institui o Plano Nacional de Informática e Automação e o Fundo Especial de Informática e Automação.”

Outra Lei importante é a 96.036, de 12 de maio de 1988, que “regulamenta a Lei n° 7.646, de 18 de dezembro de 1987 que dispõe sobre a proteção da propriedade intelectual de programas de computador e sua comercialização no País.” Sem falar na Lei 9.983, de 14 de julho de 2000, que altera o Código Penal Brasileiro em alguns artigos. Há ainda outras leis sobre informática no Brasil. Mas não uma que prevê condutas específicas caracterizadoras de crimes de informática.

Com relação ao tratamento dos crimes de informática em outros países do mundo, ressalta Fabrizio Rosa que “são poucos os países que possuem uma legislação adequada sobre a criminalidade informática”. O Conselho Europeu ocorrido em 03 de setembro de 1989 estabeleceu tipos penais nos quais se basearam as legislações de países como Austrália, Alemanha, Portugal, França e Grécia, por exemplo (ROSA, 2002).

## 3 O DIREITO DE INFORMÁTICA E O CRIMINOSO DIGITAL

Inicialmente é importante fazer uma pequena abordagem a respeito do chamado Direito de Informática. Ele se constitui como sendo o conjunto de aspectos jurídicos que envolvem a internet. Esse novíssimo ramo do Direito se faz presente a partir da necessidade de regular as diversas relações que envolvem a aplicação da informática. Nesse sentido, a Informática Jurídica se divide em

dois ramos diferentes, conforme elenca Fabrício Rosa: o Direito Civil da Informática e o Direito Penal da Informática (ROSA, 2002).

Regulando as ações privadas na web estaria o Direito Civil da Informática, normatizando, por exemplo, a questão do direito autoral. Enquanto que a respeito da prevenção e punição do mau uso da rede, estaria a cargo do Direito Penal Informático, responsável, por exemplo, por conter condutas criminosas, tais como lavagem de dinheiro, calúnia, difamação, furto de informações, dentre outras.

À medida que a internet provém uma enorme gama de recursos de comunicação, entretenimento e informação, tudo de forma muito célere, também torna-se meio de induzimento e prática de infrações penais. A utilização de computadores e da maior rede de comunicação do mundo, a internet, expõe uma nova modalidade criminosa: os crimes de informática.

Nesse sentido, importante se faz mencionar a figura do “Criminoso Digital”. São os *crackers*, expressão usada para designar os sujeitos que roubam arquivos, invadem redes, furtam informações e violam sistemas cibernéticos. Há também os *hackers*. Fabrício Rosa faz essa importante distinção, definindo quem são essas pessoas que atuam ilicitamente na rede.

*Hackers são aqueles que [...] tem conhecimentos profundos de sistemas operacionais e linguagens de programação. Conhecem as falhas de segurança dos sistemas e estão sempre à procura de novas falhas. Invadem sistemas pelo prazer de provar a si mesmos que são pessoas capazes; sem alterar nada (ROSA, 2002).*

Os *crackers* se diferem dos *hackers* por utilizarem seu conhecimento para o “mal”. Conforme expende o professor Fabrício, destruir e roubar são as palavras de ordem destas pessoas. Dessa forma, o *cracker* usa seus conhecimentos para obter alguma vantagem; roubando informações sigilosas para fins próprios e destruindo sistemas para si exibir.

Outros criminosos do ambiente informático são o *preaker* e o *lammer*. O primeiro corresponde àquele que “atua na obtenção de ligações telefônicas gratuitas e instalação de escutas. São os especializados em telefonia. Utilizam-na como meio para facilitar o ataque a sistemas a partir de acesso exterior, de forma a ficarem invisíveis ao rastreamento ou a colocar a responsabilidade em terceiros” (ROSA, 2002),

Já o *lammer* é aquela pessoa que, segundo Fabrício, está tentando ser *hacker*. É o iniciante. Indaga à todos sobre o que fazer para tornar-se um. Nesse sentido, possui um pouco de conhecimento sobre invasão de sistemas. Ainda há o guru ou o “mestre dos *hackers*” que é quem possui conhecimentos superiores e grande domínio sobre todos os tipos de sistemas (ROSA, 2002).

Mister se faz ressaltar que não há um perfil determinado para o criminoso digital. Ao contrário do que muitos pensam, não é necessário ser um especialista para cometer infrações penais na internet. Com a popularização cada vez maior do acesso à rede, alguém com um conhecimento ainda que incipiente sobre informática é potencialmente capaz de cometer crimes no ambiente virtual.

Com relação ao sujeito passivo desses crimes, tem-se que pode ser qualquer pessoa, natural ou jurídica, de natureza pública ou privada. Com tudo, sabe-se também que a maioria dos crimes cibernéticos não chegam ao conhecimento da autoridade competente, fato este que impede, consideravelmente, a apuração desses delitos e a conseqüente punição dos responsáveis.

#### **4 ATUAÇÃO DAS AUTORIDADES COMPETENTES: PROMOTORIAS E DELEGACIAS**

Criada em 16 de junho de 2008, por meio da Resolução nº 56, a Promotoria Estadual de Combate aos Crimes Cibernéticos “tem o objetivo de capacitar e prestar apoio técnico, além de articular ações conjuntas com os órgãos de execução ministeriais de todo o Estado no enfrentamento dessa nova modalidade delitiva.”

Segundo estatísticas, a Promotoria de Combate aos Crimes Cibernéticos informa que as principais vítimas das infrações penais cometidas por meio da rede são as crianças e os adolescentes; tendo como principal motivo o não acompanhamento dos pais com relação ao acesso dos filhos à internet.

Para informar e orientar a cerca dos perigos da web, a Promotoria se engaja também na distribuição de cartilhas informativas e realização de palestras e demais eventos direcionados à prevenção desses crimes. Atualmente, a maior iniciativa do Ministério Público é com relação ao combate à pornografia infantil, crime grave que mais acomete os jovens internautas.

A Promotoria de Combate aos Crimes Cibernéticos de Minas Gerais localiza-se em Belo Horizonte e possui uma página na rede ([www.mp.mg.gov.br](http://www.mp.mg.gov.br)) na qual disponibiliza importantes informações de prevenção aos crimes cibernéticos e de como atuar nos casos de ser vítima destas infrações.

Como se sabe, a Promotoria de Combate aos Crimes Cibernéticos é o órgão competente para propor Ação Penal Pública Incondicionada e Pública Condicionada a Representação e Ação Penal de iniciativa Privada, todas relacionadas a crimes informáticos.

Exemplos de crimes cuja ação não exige nenhuma condição para que o Ministério Público possa iniciá-la ou requisitar a instauração de inquérito policial são: Apologia/incitação ao crime (arts. 286 e 287 do CP), Constrangimento ilegal (art. 146 do CP), Dano (art. 163 do CP, exceto se for por motivo egoístico ou com prejuízo considerável), Estelionato (art. 171 do CP), Estorsão (art. 158 do CP), Induzimento, instigação ou auxílio ao suicídio (art. 122 do

CP), Favorecimento à prostituição (art. 228 do CP), Pedofilia (art. 241 do Estatuto da Criança e do Adolescente), Propaganda eleitoral fora de época (art. 36 da Lei 9504/97), Racismo (art. 20 da Lei 7716/89), Rufianismo (art. 230 do CP), Tráfico (art. 33 da Lei 11343/06), Tráfico de pessoas (art. 231 do CP) e Violação do Direito Autoral (art. 184 do CP).

Nos casos em que é exigida manifestação de vontade da parte ofendida para o Ministério Público iniciar a ação penal ou para que as investigações policiais sejam iniciadas, são exemplos os seguintes crimes: Ameaça (art. 147 do CP, Corrupção de menores (art. 218 do CP), Crime contra a honra de funcionário público em razão de suas funções (art. 141, I, c/c art. 145, parágrafo único do CPP) e Violação de comunicação telegráfica, radioelétrica ou telefônica (art. 151 do CP).

Por fim, como exemplos de crimes de ação penal privada, isto é, aquela em que o direito de promover a ação pertence ao ofendido ou a quem de direito possa representá-lo, listam-se os seguintes crimes: Injúria (art. 140 do CP), Difamação (art. 139 do CP), Calúnia (art. 138 do CP) e Dano por motivo egoístico ou com prejuízo considerável à vítima, (art. 163, IV do CP). Importante ressaltar que os delitos de ação penal privada é necessário que o ofendido (ou seu representante legal) mova a ação, com o auxílio de um advogado.

A Delegacia Especializada em Crimes Cibernéticos em Minas Gerais é DEICC (Delegacia Especializada em Investigações de Crimes Cibernéticos) também localizada em Belo Horizonte. Com efeito, não há uma legislação específica para regulamentar os cibercrimes, mas isso não impede o desenvolvimento do trabalho da polícia.

## 5 CASOS CONCRETOS E ABORDAGENS JURISPRUDENCIAIS

Tem se tornado comum no cotidiano de todos, ouvir falar sobre casos de crimes cometidos por meio da internet. Ocorrências de pedofilia, racismo, maus tratos com pessoas e animais, calúnias, ameaças, enfim, todo tipo de delitos. Nesse sentido, importante é mencionar alguns casos concretos e julgados que envolvem a aplicação da atual legislação criminal.

Conforme a página na internet do Ministério Público Estadual, “denúncias de pornografia infantil na web ultrapassaram 25 mil no Brasil em agosto de 2009. No primeiro semestre daquele ano, a ONG Safernet recebeu 25.212 denúncias referentes à pornografia infantil na internet. Desse conteúdo, cerca de 40% das páginas foram removidas pelos provedores responsáveis pelos serviços por conterem indícios suficientes de crime por violação a termo de uso. As informações foram divulgadas por meio de um comunicado do Ministério Público Federal de São Paulo, no dia três de agosto de 2009”.

“Foram encaminhadas cerca de 1.926 notícias e imagens com indícios de pornografia infantil veiculadas na rede social

Orkut. Desse número, 1.287 resultaram em pedidos de quebra de sigilo pelo Ministério Público e outros ainda continuam sob investigação. Ainda de acordo com a Procuradoria, foram ainda instaurados 263 inquéritos policiais, 174 na capital e 89 no interior do Estado de São Paulo. A Procuradoria instaura um procedimento e, se for o caso, envia ao Ministério Público Federal de outras localidades somente depois de descobrir a cidade aonde foi cometido o possível crime”.

No Rio Grande do Sul, “o Ministério Público denunciou quatro jovens acusados de matar um cachorro a pauladas em Balneário de Quintão. O caso se tornou público porque o grupo filmou a ação e divulgou o vídeo na internet pelo portal «Youtube». Eles foram denunciados por maus-tratos e, se condenados, poderão ficar presos por até um ano, segundo informações da Promotoria”.

Em outro caso, “quadrilha é denunciada por fraude em vendas pela internet. Conforme informações do Ministério Público, quatro homens foram denunciados por estelionato nesta segunda-feira. Segundo o Ministério Público Estadual, o grupo representava uma empresa que aplicava golpes na venda de equipamentos eletrônicos pela internet. Após receberem o dinheiro, os produtos não eram entregues”.

## 6 A QUESTÃO MIDIÁTICA E A REPERCUSSÃO SOCIAL

O ser humano, durante a sua evolução histórica, passou por diversas mudanças. A forma de se comunicar foi uma dentre as várias mudanças que ocorreram com ele. O homem sente a necessidade de se comunicar depois que começou a viver em sociedade, fosse para alertar sobre alguma coisa ou expressar sua cultura ou sentimento. A partir do momento em que ele deixa de ser sedentário e passa a ser nômade, a comunicação adquire um papel significativo para a sua sobrevivência.

Por ser um processo dinâmico e evolutivo a comunicação inventa mecanismos que facilitam o entendimento da mensagem enviada pelo emissor ao receptor. O primeiro mecanismo criado que permitiu a troca de informações de maneira mais inteligível foi a escrita. Essa forma codificada promoveu a possibilidade de tornar a informação acessível a um número cada vez mais crescente de pessoas, alterando assim o modo de viver e de pensar de uma sociedade. Com o ensejo de informar o público sobre os mais importantes acontecimentos sociais e políticos surge o jornal, um método primitivo, mas que continua sendo utilizado pela sociedade contemporânea diante da era informatizada.

Através da necessidade de expandir o novo modelo econômico e divulgá-lo de maneira mais rápida para uma maior quantidade de pessoas foi criado mais um mecanismo de comunicação: o rádio. O rádio propagou as diretrizes do capitalismo impulsionado pela Revolução Industrial, pois suas ondas tinham um alcance e

velocidade muito superiores atingindo o objetivo desse novo modelo de produção: a cultura de massa. Essa revolução fez com que o homem abandonasse a sua vida no campo e passasse a compor o cenário liberal. A partir de agora, o homem começa a manipular uma máquina e estar por detrás dela.

Com este modelo capitalista, a humanidade, em constante evolução, passa por uma grande mudança: deixar de ser uma civilização agrícola para ser uma civilização industrial. Através da ideologia da “nova” civilização, que se estrutura na cultura em massa, juntamente com os dois mecanismos de comunicação anteriormente criados, a escrita e o rádio, ocorre a junção dos componentes gráficos com os componentes de áudio sendo assim possível ver imagens em movimento juntamente com o som. Surge assim a televisão, um novo meio de comunicação, que permite um tráfego crescente de informações e que propiciará o surgimento da Era da Informação.

As transformações que aconteceram com o surgimento da televisão e sua disseminação da informação permitiram com que o homem criasse e vivenciasse uma nova era, a Era da Informação. “É com o surgimento da tecnologia digital, culminando na criação da Internet,” que permite a consolidação dessa era, “pela inclusão de dois novos elementos: a velocidade, cada vez maior na transmissão de informações, e a origem descentralizada desta” (PINHEIRO, 2008).

De acordo com Patrícia Peck, na obra Direito Digital:

*A sociedade humana vive em constante mudança: mudamos da pedra talhada ao papel, da pena com tinta ao tipógrafo, do código Morse à localização por Global Positioning System (GPS), da carta ao e-mail, do telegrama à videoconferência. Se a velocidade com que as informações circulam hoje cresce cada vez mais, a velocidade com que os meios pelos quais essa informação circula e evolui também é espantosa (PINHEIRO, 2008).*

É diante da velocidade proporcionada pela Internet que ela acabou conquistando o seu devido espaço na sociedade. Todos os fatores que estruturam a sociedade (social, econômico e político) permitiram a sua expansão e ela tornou um meio essencial de comunicação da sociedade, tudo agora está vinculado à Internet. A internet passa a ser um veículo de informação de repercussão mundial. “A Internet elimina definitivamente o conceito de corporação unidimensional, impessoal e massificada. Isso significa profunda mudança na forma como o Direito deve encarar as relações entre esses Indivíduos” (PINHEIRO, 2008).

Em um mundo globalizado, o acesso as informações se tornou uma questão primordial, a presença da diversidade está em destaque e com isso, os sistemas que regulam essa pluralidade

devem ser modificados. E como integrante desses sistemas, o Direito, não poderia ignorar tal realidade e, por isso, os seus operadores vêm utilizando a Internet de maneira cada vez mais habitual. A distância que existia entre os profissionais da área jurídica e os serviços disponíveis na Internet está cada vez menor, pois em um curto espaço de tempo é possível se obter informações que, sem ela se levava horas, ou até mesmo dias.

Através da facilidade e rapidez com que a Internet proporcionou a essa sociedade acessar diversos conteúdos, ao mesmo tempo, ela também permitiu a integração dessa sociedade através da criação das redes sociais. Essas redes sociais concedem ao indivíduo a possibilidade de se expressar. Mas ao exprimir um sentimento estando conectado pode resultar em uma repercussão na sociedade, às vezes, sem limites. Essa é a grande diferença da era industrial da era da informação a responsabilidade civil diante da informação veiculada.

*A Sociedade Digital já não é uma sociedade de bens. É uma sociedade de serviços em que a posse da informação prevalece sobre a posse de bens de produção. Essa característica faz com que a proteção do Direito à Informação seja um dos princípios basilares do Direito Digital, assim como a proteção de seu contradireito, ou seja, do Direito à não informação (PINHEIRO, 2008).*

Portanto, para se obter uma responsabilidade civil consciente é necessário que os usuários da rede a utilizem não só de forma quantitativa, mas também de forma qualitativa, ou seja, “informação autêntica com responsabilidade editorial pelo conteúdo” (PINHEIRO, 2008). É por isso que o Direito, sistema regulador e normeador da sociedade, atinge a esfera social virtual e através da sua força normativa estabelece alguns freios, mas ainda insuficientes diante da facilidade e velocidade que se propaga a informação.

## **7 O COMETIMENTO DE CIBERCRIMES POR MEIO DE REDES SOCIAIS**

### **7.1 REDES SOCIAIS: CONCEITO**

As redes sociais são um meio de se conectar a outras pessoas na internet criando laços cibernéticos. São páginas da web que facilitam a interação entre seus membros, independentemente de onde eles estejam. Os sites das redes sociais geralmente funcionam tendo como base os perfis de usuário - uma coleção de fatos sobre o que um usuário gosta, não gosta, seus interesses, *hobbies*, escolaridade, profissão ou outro dado que ele queira compartilhar.



O objetivo do participante de uma rede social é se conectar com pessoas e, dessa forma, estabelecer comunicação; é se juntar a um grupo de pessoas com quem compartilhe um *hobby* ou um interesse, a fim de fazer amizades e adquirir contatos.

## 7.2 Espécies

No Brasil, há três espécies de redes sociais mais acessadas: o *Orkut*, o *Facebook* e o *Twitter*. O *Orkut* é o conjunto de perfis de pessoas e suas comunidades, ou seja, grupos que compartilham algum interesse em comum. Nele, é possível cadastrar-se e postar fotos e preferências pessoais, além de listar amigos e participar das mencionadas comunidades. Criado por Orkut Buyukokkten, ex-aluno da Universidade de Stanford, esta rede social foi lançada pela *Google*, em janeiro de 2004.

O *Facebook* se assemelha bastante ao *Orkut*. Fundado por Mark Zuckerberg, Eduardo Saverin e Chris Hughes, ex-estudantes da Universidade de Harvard, o *Facebook* inicialmente era uma rede social usada somente por alunos daquela Universidade. Atualmente, a rede tem cerca de 750 milhões de usuários, vindo, inclusive, a se tornar tema de filme, neste ano de 2011: “A rede social”, filme este cujo enredo narra a sua criação e o suposto plágio de Mark Zuckerberg.

O *Twitter*, por sua vez, é um microblog de informação em tempo real que conecta seus participantes às últimas informações postadas. Assim como nas demais redes sociais, no *twitter* também há perfis em que as pessoas “seguem”, caso se identifiquem ou gostem das idéias postadas. O *Twitter* é composto por pequenas mensagens de informação chamadas *tweets*. Cada *tweet* tem até 140 caracteres. O *Twitter* está sediado em São Francisco, EUA, mas é utilizado por pessoas de quase todos os países. Ele está disponível em inglês, francês, alemão, italiano, japonês e espanhol. O microblog *Twitter* conseguiu adentrar a Praça de São Pedro no Vaticano e até o papa Bento XVI é um ilustre usuário da rede social.

## 7.3 A era da informação e o acesso às redes sociais

Quando se cria uma rede social, elas tendem a funcionar como redes de relacionamentos no mundo real, porém podem ser utilizadas para forjar laços sociais. Com uma observação mais detalhada, percebe-se que a maioria das “distâncias” entre os membros do sistema é reduzida pela presença de alguns indivíduos, que são “amigos de todo mundo”.

É fácil percebê-los; são as pessoas conectadas com um imenso número de amigos. Enquanto a maioria dos perfis no *Orkut* tem, no máximo, 400 amigos, algumas pessoas, como o brasileiro Roger Jones ou o americano Adam Rifkin, alcançaram algo em torno de mil amigos. Isto constata que a maioria dessas conexões é falsa, no sentido de que não apresenta nenhum tipo de interação

social. Trata-se simplesmente de uma “coleção” de perfis.

O acesso às redes sociais atualmente é regra para jovens e esta nova geração de executivos declara que prefere as redes sociais na hora de procurar um novo emprego. É o que revela a pesquisa que mostra que 65% dos profissionais com idade entre 26 e 30 anos preferem as redes sociais e os sites para procurar informações sobre oportunidades de carreira. Dos participantes da pesquisa com mais de 40 anos, 48% afirmaram que usam as ferramentas *online* para encontrar novas opções de emprego. As redes sociais deverão se consolidar também como um importante canal de atendimento ao consumidor.

A coleta de informações por meio de *sites* de relacionamento tem se tornado comum. Isso porque órgãos privados e públicos têm se beneficiado de informações publicadas em sites, blogs e redes sociais, por serem de fácil acesso. Toda informação pública disponível pode ser utilizada, o que torna os internautas alvo fácil dos criminosos digitais.

## 7.4 O que fazer diante um cibercrime

Rotineiramente, ocorrem fatos desagradáveis na internet como a perda ou furto de perfis em redes sociais. O Ministério Público do Estado disponibiliza em seu portal dicas de como agir quando alguém for vítima dos crimes cometidos por meio de redes sociais. No caso, por exemplo, de roubo de senhas dos perfis, cópia de fotos para serem utilizadas em *sites* pornográficos e clonagem de perfis é necessário comunicar a central de ajuda da rede social e relatar o ocorrido.

As informações serão checadas e, caso verdadeiras, a conta na rede social será excluída. Se o furto ou perda não forem resolvidos por este meio é necessário acionar o Poder Judiciário. É preciso verificar quem é o responsável pela rede social no Brasil e depois consultar um advogado ou um defensor público para iniciar na tomada de providências.

Deve-se ter em mãos todas as páginas impressas de forma a comprovar que a rede social foi perdida ou furtada. O advogado que propor o procedimento pode pedir uma antecipação de tutela para “retirar do ar” o perfil da rede social.

É necessária cautela também na hora de abrir *e-mails* que se dizem ser de instituições públicas e bancos. A recomendação, nesses casos, é a de não abrir o mencionado *e-mail* e não clicar em qualquer outro *link* antes de entrar em contato com a instituição que supostamente o enviou confirmar o envio.

Ante o exposto, é preciso cuidado ao acessar e participar das redes sociais de forma a ter discernimento com relação a informação a ser exteriorizada através da postagem, haja vista as consequências poderem ser insanáveis.

## 8 CRIMES INFORMÁTICOS: CARACTERÍSTICAS

Atualmente, foi noticiado em diversos meios de comunicação que *hackers* publicaram em perfis do *Twitter links* que supostamente conteriam dados pessoais como CPF, PIS, data de nascimento e telefones da atual Presidenta da República, Dilma Rousseff e do então prefeito de São Paulo Gilberto Kassab. A partir desse fato, surge então a dúvida sobre crimes cometidos na rede. Quais as leis que os disciplinam, sua classificação, os elementos da conduta típica, o tempo e o local do delito?

Segundo o professor Doutor Túlio Vianna, há dois conceitos de crime, considerando o conceito formal de delito, no qual “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, (art. 1º do Código Penal Brasileiro). O acesso não autorizado a computadores seria considerado atípico. Porém, partindo do pressuposto de que há lesão ou perigo de lesão a um bem jurídico, no caso deste ilícito o bem jurídico tutelado seria o direito a privacidade (VIANNA, 2003).

Importante ressaltar que o bem jurídico tutelado pelas normas que disciplinarem os crimes cometidos na internet não seria a inviolabilidade dos programas, mas sim o acesso não autorizado a informações e dados pessoais. Não se pode classificar como crimes informáticos todos aqueles em que o computador for utilizado como meio para prática do delito (VIANNA, 2003).

Expende o professor que “A simples utilização por parte do agente de um computador para a execução de um delito, por si só não configuraria um crime informático” (VIANNA, 2003). Ele classifica os crimes informáticos em impróprios (aqueles nos quais o computador é empregado como instrumento, mas não há ofensa ao bem jurídico tutelado) e os próprios (aqueles crimes nos quais há lesão ao bem jurídico tutelado).

Os crimes informáticos impróprios geram bastante repercussão, pois não necessitam por parte do autor de conhecimentos técnicos, específicos. À exemplo, uma relação afetiva entre um casal; ao se separar, um dos cônjuges, insatisfeito com o fim do romance resolve publicar em redes sociais declarações ofensivas a respeito do outro cônjuge. Ou seja, utilizando-se do meio digital, tal pessoa pratica crimes como calúnia e difamação muito bem classificados no atual Código Penal Brasileiro. No mencionado caso, não há inviolabilidade ao bem jurídico tutelado, portanto seria classificado como crime informático impróprio.

E os crimes informáticos próprios? Um exemplo seria a Lei nº 9.983/2000 que acrescentou ao Código Penal Brasileiro as hipóteses de acesso a dados por funcionário público no exercício de suas funções.

Noutro giro, é importante determinar o momento da ocorrência do crime informático. O atual Código Penal Brasileiro, em

seu artigo 4º, estabelece que “Considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado” (art. 4º do Código Penal Brasileiro). Nesse sentido, observa-se que nos crimes informáticos o período entre a ação e o resultado podem ser duradouros. Um exemplo que o professor Túlio Vianna analisa, é o caso de transferência de arquivo que pode levar horas ou talvez dias. Nesse caso, o delito é praticado no momento em que for dado o comando de transferência.

No que tange ao local do crime o Código Penal transpõe: “Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”(art. 6º do Código Penal Brasileiro). Nesse aspecto, há uma questão polêmica a respeito do local em que se pratica o crime. Suponha-se que o crime seja cometido em países diferentes; em qual desses países seja considerado atípico? “Havendo duas interpretações possíveis perfeitamente lógicas para uma mesma situação jurídica, deve o intérprete optar por aquela que menos restringir a liberdade do cidadão”.

## 9 INTIMIDADE, PRIVACIDADE X INTERNET: APROXIMAÇÕES E DISTANCIAMENTOS

A Constituição Federal do Brasil, em seu artigo 5º, inciso X, dispõe:

*Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]*

*X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.*

É a partir da Carta Maior que os demais ramos do Direito se constituem. Estruturados e delimitados pelos princípios da Constituição Federal esses ramos tutelam tanto os direitos coletivos como também os direitos privados. Sendo mais uma dessas ramificações, o Direito Digital está vinculado aos pressupostos constitucionais por possuir ainda uma legislação incipiente.

De acordo com Dicionário Houaiss, intimidade é a “*relação de caráter que é íntimo, é a familiaridade, privacidade*”. E a definição de privacidade é “*a intimidade, é a particularidade, pessoalidade, privatividade*”. Esses verbetes possuem essas definições, mas diante da linguagem jurídica eles adquirem outra roupagem. Esses dois conceitos compõem os Direitos da Personalidade que tem por objeto os atributos físicos, psíquicos e morais da pes-

soa em si e em suas projeções sociais. São inerentes às pessoas e, portanto a elas ligados de maneira perpétua e permanente.

A Internet e esses conceitos supracitados irão possuir pontos convergentes no momento em que ela for tratar do indivíduo como aquele que está por detrás do computador manipulando a rede, expondo e utilizando, às vezes de maneira exacerbada, a sua liberdade de expressão. A partir do momento que o indivíduo utiliza-se dessa liberdade e propaga determinada opinião ele passa a se vincular com todos os demais indivíduos que compõe essa rede interligada de maneira interminável. Ao mesmo tempo em que ele se encontra sozinho, vivendo uma relação de intimidade, ao se conectar o mesmo fica interligado com dezenas de pessoas, em suas redes sociais, perdendo assim o caráter desta relação de privacidade, intimidade ao exteriorizar um pensamento.

A velocidade com que ocorre a transmissão das informações pela Internet conquistou todo o mundo. Devido a esta característica, a Internet passou a ser considerada um meio de comunicação de cultura em massa. Associando essas características, velocidade e cultura em massa, com os conceitos de privacidade e intimidade ocorrerre uma colisão provocando distanciamentos, ou seja; o mau uso na transmissão de informações agregado ao excesso da exteriorização da privacidade e intimidade podem acarretar diversas conseqüências que serão tuteladas pelo Direito Digital.

As conseqüências do comportamento dos usuários da Internet, ao divulgar qualquer tipo de informação na rede, devem ser sempre rodeadas de discernimento. Um simples “enter” pode destruir carreiras, relacionamentos, pois ao propagar a informação e vincular diversas pessoas na rede sem que elas tenham conhecimento disso fazem com que o coletivo sobreponha ao individual. Portanto, ao divulgar qualquer tipo de conteúdo é necessário seguir o velho conselho e “pensar duas vezes”.

## 10 PROPOSTAS PARA UMA UTILIZAÇÃO ADEQUADA DAS REDES SOCIAIS

O hoje, em se tratando de tecnologia, já virou passado. O computador usado ano passado já não é tão bom quanto o utilizado nos dias atuais e assim será sucessivamente. A informação chega em questão de segundos. Uma página com vírus aberta, um comentário postado em redes sociais pode tornar-se fatal na vida de qualquer um. Não é exagero: a velocidade com que se tem acesso a informações pessoais é assustador, principalmente após o advento das já mencionadas redes sociais.

Por isso é importante atenção e certas precauções diante a tela do computador, na qual está representado um mundo tão dinâmico. Iniciativas simples como o fato de não revelar a senha a ninguém, ou não usar caracteres conhecidos como senha, (data de aniversário, números de telefone, enfim), não fornecer dados pes-

soais a estranhos, não abrir *emails* de remetentes desconhecidos ou não marcar encontros com pessoas conhecidas na rede são iniciativas importantes para se evitar tornar-se vítima dos *cibercrimes*. Além disso, não publicar fotos que permitem identificar onde se mora ou não postar comentários inadequados que expressem sentimentos que podem ser interpretados como preconceitos são essenciais em se tratando de utilização segura da internet.

Tudo o que é postado na internet, pode ser acessado a qualquer momento, ainda que se tenha retirado ou “apagado” este conteúdo da rede. Os poucos minutos em que a informação postada esteve “no ar” já foi suficiente para que inúmeras pessoas de todo o mundo tivessem acesso e, portanto, para que reproduzissem o que foi inadequadamente “postado”. Desta forma, criando constrangimentos para o sujeito remetente da informação ou até mesmo proporcionando chances para que o “criminoso digital entre em ação”.

É importante ressaltar ainda que quando se acessa a internet, esse mundo virtual, se está sujeito à normas semelhantes àquelas em que respeitamos no mundo real. Na internet, os internautas deixam de ser anônimos quando desrespeitam o direito de uma outra pessoa. Nesse sentido, é preciso saber que, mesmo não havendo uma legislação específica para crimes cometidos na rede, a internet não é uma terra sem lei. Ela representa uma quebra de fronteiras, uma verdadeira revolução tecnológica na sociedade, logo, não pode ser usada como uma ferramenta para a prática de atos ilegais. E isso será determinado através da sua apropriada utilização por todos os que a acessam.

## 11 CONCLUSÃO

Revela-se com o trabalho a existência de um novo ramo do Direito, qual seja, o Direito de Informática, surgido no contexto em que a internet passa a ser utilizada não só como uma ferramenta para o desenvolvimento da sociedade, mas também no cometimento de atos ilícitos; os chamados crimes cibernéticos.

Nesse sentido, adviram problemas jurídicos tais como a ausência de uma legislação penal autônoma e específica para regulamentar os delitos da internet. Contudo, isso não significa que a internet é uma “terra sem lei”. Ademais, também não impede o trabalho dos órgãos competentes em articular ações no enfrentamento dessa nova modalidade delitiva.

Outrossim, é necessário estabelecer diretrizes para o uso seguro da internet, principalmente no que tange a participação em redes sociais.

Há importantes precauções a serem tomadas; a apropriada utilização da rede por todos os que a acessam é meio eficaz no combate ao criminoso digital.

Ante o exposto, verifica-se que a falta de uma previsão legal das condutas cibernéticas ilegais pode levar a desconfortável idéia



de impunidade, mas toda a sua dificuldade em legislar está associada a rapidez com que as informações se propagam fruto de mundo intocável.

## REFERÊNCIAS

ALMEIDA FILHO, José Carlos de Araújo; CASTRO, Aldemário Araújo. *Manual de informática jurídica e direito da informática*. Rio de Janeiro: Forense, 2005.

BRASIL, *Código Penal Brasileiro (Código Penal)*. Brasília: Senado: 1940.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. 10ª. ed. São Paulo: Rideel.

BRASIL. Decreto nº 96.036, de 12 de maio de 1988. Regulamenta a Lei nº 7.646, de 18 de dezembro de 1987 que dispõe sobre a proteção da propriedade intelectual de programas de computador e sua comercialização no País, e dá outras providências.

BRASIL. Lei nº 9.983, de 14 de julho 2000. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências.

BRASIL. Lei nº 7234, de 29 de outubro de 1984. Esta Lei estabelece princípios, objetivos e diretrizes da Política Nacional de Informática, seus fins e mecanismos de formulação, cria o Conselho Nacional de Informática e Automação - CONIN, dispõe sobre a Secretaria Especial de Informática - SEI, cria os Distritos de Exportação de Informática, autoriza a criação da Fundação Centro Tecnológico para Informática - CTI, institui o Plano Nacional de Informática e Automação e o Fundo Especial de Informática e Automação.

CASTELLS, Manuel. *A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade*. Rio de Janeiro: J. Zahar, c2003. 243p.

CORRÊA, Gustavo Testa. *Aspectos jurídicos da Internet*. 3. ed. São Paulo: Saraiva, 2007.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto. *Direito e internet: aspectos jurídicos relevantes*. São Paulo: Edipro, 2000.

Disponível em <<http://www.mp.mg.gov.br/portal/public/interno/index/id/10>> Acesso em 09 de ago. 2011.

Disponível em <<http://facebook.com>> Acesso em 30 de jul. 2011.

Disponível em <<http://h30458.www3.hp.com/br/ptb/smb/941786.html>> Acesso em 06 de jul. 2011.

Disponível em <<http://info.abril.com.br/noticias/carreira/rede-social-e-1-opcao-na-busca-por-emprego-27042011-24.shl>> Acesso em 06 de jul. 2011.

Disponível em <<http://orkut.com.br>> Acesso em 30 de jul. 2011.

Disponível em <<http://twitter.com>> Acesso em 30 de jul. 2011.

Disponível em <<http://www.blogdacomunicacao.com.br/rede-social-na-internet-o-que-e-isso/veja.abril.com.br/080709/nos-lacos-fracos-internet>

-p-94.shtml> Acesso em 06 de jul. 2011.

Disponível em <[http://www6.ufrgs.br/limc/PDFs/redes\\_sociais.pdf](http://www6.ufrgs.br/limc/PDFs/redes_sociais.pdf)> Acesso em 06 de jul. 2011.

FERREIRA, Lóren Formiga de Pinto. *Os crimes de informática no Direito Penal Brasileiro*. Disponível em <[http://www.ambitojuridico.com.br/site/index.php?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=6064](http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6064)> Acesso em 05 de jul. 2011.

GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva. *Direito e Internet: relações jurídicas na sociedade informatizada*. São Paulo: Revista dos Tribunais, 2001.

GRECO, Rogério. *Código Penal Comentado*. 5. ed. Niterói, Rio de Janeiro: Impetus, 2011, 1098.

PINHEIRO, Patrícia. *Direito Digital*. 2. ed. São Paulo: Saraiva, 2008.

ROSA, Fabrício. *Crimes de Informática*. 1. ed. Campinas, São Paulo: Book-seller, 2002.

ROVER, Aires José (Org.). *Direito, sociedade e informática: limites e perspectivas da vida digital*. Florianópolis: Fundação Boiteux, 2000.

ROVER, Aires José. *Direito e informática*. Barueri, SP: Manole, 2004.

SCHOUERI, Luís Eduardo (Org.). *Internet: o direito na Era Virtual*. 2. Ed. Rio de Janeiro: Forense, 2001.

VIANNA, Túlio Lima. *Fundamentos de direito penal informáticos: do acesso não autorizado a sistemas computacionais*. Rio de Janeiro: Forense, 2003.

## NOTAS DE FIM

1 Graduanda em Direito pela Faculdade Mineira de Direito da PUC/Minas.

2 Graduanda em Direito pela Faculdade Mineira de Direito da PUC/Minas.

3 Graduanda em Direito pela Faculdade Mineira de Direito da PUC/Minas.

4 Graduanda em Direito pela Faculdade Mineira de Direito da PUC/Minas.

5 Doutorando em Direito pela Pontifícia Universidade Católica de Minas Gerais. Mestre em Direito pela Pontifícia Universidade Católica de Minas Gerais. Especialista em Processo Civil Aplicado pelo CEAJUFE/IEJA. Bacharel em Administração pela Pontifícia Universidade Católica de Minas Gerais. Bacharel em Direito pela Universidade José do Rosário Vellano. Professor e Pesquisador da Faculdade Mineira de Direito da Pontifícia Universidade Católica de Minas Gerais. Professor do Centro Universitário Newton Paiva. Professor da Universidade Presidente Antônio Carlos. Membro associado do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI). Membro colaborador do ICP (Instituto de Ciências Penais), do IBCCRIM (Instituto Brasileiro de Ciências Criminais), do IBDP (Instituto Brasileiro de Direito Processual), do IBDP (Instituto Brasileiro de

Direito Público), do IBDC (Instituto Brasileiro de Direito Constitucional), do IDC (Instituto de Direito Civil), do IDEC (Instituto de Defesa do Consumidor) e do IBDFAM (Instituto Brasileiro de Direito de Família). Integrante dos Grupos de Pesquisas: Direito, Constituição e Processo “José Alfredo de Oliveira Baracho Júnior” e Direito, Sociedade e Modernidade “Rita de Cássia Fazzi”. E-mail para contato: cristiankiefer@yahoo.com.br